Computer Network Defense (CND) Team Services Catalog

V-Q2-2014r2 As of: 10/1/2014

Health Assessment (HA)

Service Summary: Perform a detailed asset vulnerability analysis evaluating endpoint patch management with direct correlation to NIST compliance; perform asset discovery scan of up to 4 Class "C" IP ranges.

Service Metrics: Perform Vulnerability Analysis scan on up to 150 endpoints as designed by the client. Scan to be initiated from a single client location.

Local Service $ 10,887.29 *Traveling Service* $ 18,090.87

Agency Vulnerability Assessment (TA)

Service Summary: Perform a detailed asset vulnerability analysis evaluating endpoint patch management with direct correlation to NIST compliance; perform asset discovery scan of up to 12 Class "C" IP ranges.

Service Metrics: Perform Vulnerability Analysis scan on up to 3,000 endpoints as designed by the client. Scan to be initiated from a single client location.

Local Service $ 28,448.40 *Traveling Service* $ 35,187.99

Continuous Monitoring (CM)

Service Summary: Fulfillment of a monthly reoccurring vulnerability scan service. Service consists of CND Analysts performing the collection of vulnerability information from customer endpoints. This service is provided to customers local to the Sacramento CA region. Products provided include: Asset Risk Score Trending; NIST Compliance by Month; Vulnerability Delta by Month (beginning on 2nd supported month); Remediation Report by Vulnerability, Name and Type; Operating Systems (Assets). CND Analyst analytics will not be performed by a senior analyst from the resulting scans.

Service Metrics: Pricing based on an increment of 500 endpoints. For custom pricing, please inquire. Scans to be performs from a single location. Customer responsible to ensure adequate bandwidth between the scan site and remote endpoints is provided. Client responsible to ensure endpoints are operational and responding to scans. Monthly reoccurring fees based on 12 monthly increments, subject to funding approval. Cancellations < 30 days prior notice incur 1 month reoccurring service fee cancellation charge.

Local Service $ 26,259.85 *Traveling Service* n/a

Firewall Analysis Service (FA)

Service Summary: Analyst performs Firewall Analysis & Compliance Review on specified firewall / device. Analysis and analytics will address security configuration and best practices, manageability, access controls, change management compliance (rule traceability; documented change requests, etc...); identification of overlapping or redundant rules; identification of unused rules; review firewall architecture for appropriate zone implementation, segmentation, and intercommunication; access compliance with applicable state firewall compliance rules.

Service Metrics: Performs rule analysis of exported rules for regulatory compliance, execution efficiencies, and associated risk variables on one firewall or device.

Local Service $ 16,452.23 *Traveling Service* $ 22,554.56

Notes:

- Prior editions of this document are obsolete.
- Services and pricing subject to change without notice.
- For a formal quote, please contact the CND.
- CND Catalog 2014 Q2 v2

Computer Network Defense (CND) Team Services Catalog

V-Q2-2014r2 As of: 10/1/2014

Website Vulnerability Scanner (WA)

Service Summary: An analysis of web site and the directly subordinate pages as accessed from the root or sub-site of the specified URL (e.g. www.acme.ca.gov includes www.acme.ca.gov/service, etc...). Analysis considers risk exposure regarding information disclosure, Structured Query Language Injection (SQLi) susceptibility, resistance to Cross-Site Scripting (XXS) vulnerability. The scan will not attempt to compromise the host through vulnerability exploitation.

Service Metrics: Analysis includes an external and internet scan of the site. Service addresses one site of a page depth of up to 350 pages, assessable from the location selected in the IAA.

Local Service $ 14,222.57 *Traveling Service* $ 19,957.83

Network Infrastructure Endpoint Discovery and Identification Services (IS)

Service Summary: Network discovery, mapping, inventory, and diagramming of routers ,switches, servers, wireless access point, VoIP infrastructure, systems, and printers via SNMP, WMI, and ICMP discovery process. Generation of Layer 2/3 topography maps including IP address, MAC Address, DNS Name, and Switch port connection from collected scan data. Output products are provided in multiple formats including Visio.

Service Metrics: Perform SNMP scan, device identification, and mapping of up to 1024 devices on up to 4 class C client networks.

Local Service $ 8,194.45 *Traveling Service* $ 14,075.32

Network Traffic Anomaly and Indicators of Compromise Service (IC)

Service Summary: Acquisition of raw network traffic captures from client network. Traffic will be replayed against multiple Intrusion Detection System engines and traffic analysis tools to perform a best effort analysis for the presence of Indicators of Compromise (IoC). Traffic analysis results to be provided via formal report and metrics.

Service Metrics: Collect raw network traffic from network segment as provided by the client for a period of 24 hours or up to a maximum of 250GB of data, whichever is achieved first. Due to size of captured data, traffic is destroyed by CND upon completion of analysis. If specific IoC are detected, PCAP export of specific indicator packets will be provided to the client.

Local Service $ 12,048.19 *Traveling Service* $ 17,783.45

Endpoint Malware Binary and Indicators of Compromised Binary Discovery Service (BA)

Service Summary: Performance of a Malware Binary Indicators of Possible Compromised discovery and analysis service. Using Deep Binary Assessment tools, an analysis that include hashing of binaries on the host systems, copying of registry hives, and gathering of program collections for signs on the selected systems will be collected for analysis. This analysis will attempt to determine the presence of possible malware, unapproved software, and other signs or indicators of compromise based on collected information and known indicators at the time of collection.

Service Metrics: Perform scan on up to 1500 endpoints as designed by the client. Scan to be initiated from a single client location.

Local Service $ 11,352.35 *Traveling Service* $ 16,414.88

Notes:
- Prior editions of this document are obsolete.
- Services and pricing subject to change without notice.
- For a formal quote, please contact the CND.
- CND Catalog 2014 Q2 v2